Southampton Solent University  
Computer | Science & Engineering

**“A phishing email detection model”**

Machine Learning COM624

Software Engineering BSc

2025

Daniel Weston

Tutor: Dr Taiwo Ayodele

Date of Submission: XX/XX/2025

Contents

[Introduction 3](#_Toc210144911)

[Literature Review 3](#_Toc210144912)

[Methodology 3](#_Toc210144913)

[Results 3](#_Toc210144914)

[Discussion 3](#_Toc210144915)

[Conclusion 3](#_Toc210144916)

[References 3](#_Toc210144917)

# Introduction

## Context

“Phishing scam emails are emails that pretend to be something they are not in order to get the recipient of the email to undertake some action they normally would not” (WASH, 2020). With over 4.3 billion email users worldwide sending and receiving approximately 347.3 billion emails per day (RATICATI, 2023), an estimated 1.2% of these emails are phishing attempts — roughly 3.4 billion emails daily. These attacks result in substantial financial and reputational losses; for example, the FBI reported over $4.2 billion lost due to phishing in 2023. This pervasive threat affects organizations as well, with 57% reporting phishing attacks on a weekly or daily basis (WORTHINGTON & OZSAHAN, 2024).

Detecting phishing emails is challenging due to sophisticated social engineering tactics, obfuscated URLs, and ever-evolving attack methods. Automated detection systems through the usage of machine learning techniques are therefore critical to protect both individuals and organizations. Moreover, such systems must adhere to privacy regulations by processing anonymized email content and metadata to prevent exposure of sensitive information to comply with laws such as GDPR and to build strong trust with the users by protecting their sensitive data.

## Aim

This project aims to develop a privacy-aware machine learning system capable of detecting phishing emails using real-world datasets while maintaining GDPR compliance and protecting user privacy. The system will preprocess raw email data, engineer features from both content and metadata, and train machine learning models including Random Forest and LSTM for effective phishing detection.

## Objectives

To achieve my aim, this project will:

* Build a machine learning model to detect phishing emails.
* Work with real datasets and clean them to a desired level.
* Apply privacy preserving techniques to protect user data.
* Provide visual insights and alerts via a GUI dashboard.

## Report Structure

The remainder of this report is structured as follows:

* Literature Review: Examines existing phishing detection methods and privacy-aware AI approaches.
* Methodology: Details data handling, feature engineering, and model selection.
* Results: Presents model performance, visualisations, and key findings.
* Discussion: Considers ethical, legal, and practical limitations, and outlines future work.
* Conclusion: Summarises findings and offers recommendations for future research or implementation.

# Literature Review

H

# Methodology

Je

# Results

He

# Discussion

Je

# Conclusion

E

# References

WASH 2020  
Wash, R (October 2020). *How Experts Detect Phishing Scam Emails.*Michigan State University, USA  
<https://doi.org/10.1145/3415231>

RADICATI 2023  
Radicati Group (2023). *Email Statistics Report, 2019-2023.*London, UK  
<https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf>

WORTHINGTON, OZSAHAN 2024  
Worthington, D & Ozsahan H (12th March 2024). *50+ Phishing Attack Statistics for 2025.*Jumpcloud  
<https://jumpcloud.com/blog/phishing-attack-statistics>